Attachment 1

U.S. DEPARTMENT OF COMMERCE

POLICY ON PASSWORD MANAGEMENT

What is the purpose of this policy?

This policy establishes minimum practices for management of passwords to support authentication of system users when accessing Department of Commerce (DOC) information technology (IT) systems.

To whom and to what does this policy apply?

This policy applies to all DOC personnel (federal and contractor) and all DOC IT systems or resources, independent of the size of the computer, network, device or information, including all systems using technology where passwords are used to control access. For example, it applies to desktops, laptops, servers, network devices, and networked office automation equipment. This policy also applies to those IT systems operated and used by contractors, guest researchers, collaborators, and other Federal agencies to carry out the DOC mission, whether or not they are owned, leased, or on Government property. This policy must be explicitly addressed in all IT procurement activities. Those IT systems intended to provide unrestricted access are excluded (e.g.,public Web pages and kiosks).

What does DOC require for effective password management?

This policy specifies the mandatory and recommended password management practices for all DOC IT systems. Each DOC IT system must use passwords as a means for user authentication. Systems may also use biometrics or public-key infrastructure certificates as additional means to control access. The access controls used should provide security commensurate with the level of sensitivity of the system or of specific resources (i.e., information or special devices). All DOC IT systems and associated equipment that rely on passwords as the means to authenticate users must implement effective password management in accordance with this policy.

Operating unit Chief Information Officers must identify any proposed deviations from the mandatory practices of this policy and request a waiver in writing from the DOC IT Security Manager. Approved waivers must be documented as part of the appropriate system security plan(s) that cover the system(s) applicable to the waiver. Identical systems under the same management authority and covered by one system security plan require only one waiver request.
Requests for a Password Management Waiver must:

- cite the specific mandatory practice(s) for which the waiver is requested,
- explain the rationale for the requested waiver, and
- if applicable, describe compensating controls to be in place during the period of the requested waiver, until systems are compliant with this policy, and provide an action plan (including target dates) for compliance.

Operating unit Chief Information Officers may appeal the DOC IT Security Manager's waiver decision in writing to the DOC Chief Information Officer.

Who is responsible for implementation of the DOC password management policy?

1. The DOC IT Security Manager maintains and updates the policy, reviews and approves or denies waivers, and monitors operating unit compliance through the conduct of annual compliance reviews.

2. Each DOC Head of Operating Unit must implement the mandatory practices of this policy that are not covered by an approved waiver.

1. Each DOC operating unit Chief Information Officer must implement the mandatory practices of this policy, ensure communication of the policy to system users, and ensure operating unit policy and procedures reflect these password management practices. The operating unit Chief Information Officer may develop password policies and procedures that supplement this policy to establish more stringent guidance commensurate with the level of security warranted to meet the operating unit's requirements, so long as these policies and procedures are consistent with this DOC policy.

2. Operating unit IT Security Officers must communicate this policy to all system users within the operating unit and ensure that user IT security awareness and training programs address password management. In addition, IT Security Officers should include monitoring of system user compliance with this policy as part of their periodic IT security self-assessment program or automated system evaluations, and maintain approved waivers as part of the documentation for appropriate system security plan(s).

3. Because users have primary control of password selection, all DOC employees (federal and contractor) must follow the mandatory practices of this policy in the creation and management of user passwords.

What are the mandatory practices for password management?

1. Passwords must be created consistent with the following criteria:

- Passwords must have at least eight (8) non-blank characters;

- At least one of the characters must be from the alphabet (upper or lower case);
- At least one of the characters must be a number (0-9) or a special character (e.g., ~, !, $, %, ^, and *);
- Six of the characters may only occur once in the password (e.g., ‘AAAAAAA1' is not acceptable, but ‘A%rmp2g3' and ‘A%ArmA2g3' are acceptable); <u>and</u>
- Passwords must not include any of following: vendor/manufacturer default passwords: names (e.g., system user names, family names), words found in dictionaries (i.e., words from any dictionary, spelled forward or backward), addresses or birthdays, or common character sequences (e.g., 3456, ghijk, 2468).
- Vendor-supplied default passwords, such as SYSTEM, Password, Default, USER, Demo, and TEST, must be replaced immediately upon implementation of a new system.

1. Systems or applications that have multiple passwords for different levels of access or authentication must have unique passwords for each level.

2. Passwords must be protected to prevent unauthorized use. Specifically:

- Passwords must not be shared except in emergency circumstances or when there is an overriding operational necessity as documented in an operating unit System Security Plan. Once shared, passwords must be changed as soon as possible.
- Group passwords (i.e., a single password used by a group of users) must not be used without some other mechanism that can assure accountability (such as separate and unique network User Ids).
- Group passwords must not be shared outside the group of authorized users and must be changed when any individual in the group is no longer authorized. Group passwords must never be re-used.
- Passwords that need to be shared because of an overriding operational necessity, as well as group passwords, cannot be used to control access to other IT systems or applications on IT systems.

4. Passwords in readable form (e.g., written on paper) must be kept in a safe location and not stored in a location accessible to others. For example, safe locations include storage in a locked container accessible only by the user.

5. IT systems and workstations must not display or print passwords as they are entered.

6. User applications must not be enabled to retain passwords for subsequent re-use, or be configured to bypass authentication mechanisms. For example, Internet browsers must not be enabled to save passwords for re-use.

7. Passwords must not be distributed through non-encrypted electronic mail, voice-mail, or left on answering machines.

8. Passwords must be changed as follows:

- At least every 90 days,
- Immediately if discovered to be compromised or one suspects a password has been compromised,
- Immediately if discovered to be in non-compliance with this policy, and
- On direction from management.

1. Do not reuse a password you have used any of the last 8 times you have changed your password, or more recently than 2 years from when you last used the password.

2. Access to password files or password databases must be restricted to only those who are authorized to manage the IT system.

3. If a determination is made that a password has been compromised or is not in compliance with this policy, and if the password is not immediately changed, the account must be temporarily suspended until the password is changed.

4. Passwords for servers, mainframes, telecommunications devices (such as routers and switches), and devices used for IT security functions (such as firewalls, intrusion detection, and audit logging) must be encrypted when stored electronically.

5. Passwords, other than single-use (one-time) passwords, must be encrypted when transmitted across a wide area network or the Internet.

What are the recommended practices for password management?

1. Passwords used for general access should be different than passwords used to access specific applications.

2. Passwords used to access Internet or remote systems should be different from passwords used to access internal systems and applications.

3. Passwords should be encrypted when transmitted across a local area network

4. Passwords for access to individual workstations (PCs) (such as passwords for screen savers) should be encrypted when stored electronically.

5. IT systems should be designed so that temporary User IDs, passwords, and parameters associated with other means of authentication should be designed to automatically expire after a designated date.

6. Four (4) failed attempts to provide a legitimate password for access to an IT system should result in the failed attempts being recorded in an audit log, the user being disconnected from the service, and access to be suspended for at least three (3) minutes.